III. REMARKS

Various ones of the claims were rejected under 35 U.S.C. 103 as being unpatentable over various combinations of the cited art: Talbot (US 4,411,017), Bocci (US 4,4,40,976), Morgan (US 4,229,817), Billstrom (US 5,590,133), Lewis (US 6,192,255), Kniffin (US 6,072,402), Serbetciouglu (US 5,719,918), and Kennedy (EP 0680171), as set forth in the Office Action, namely: Claims 19, 21-23, 27-29, 48, 59, 61-65, 67-69, 71-73, 77-79, 81-82, 84-85, 87, 90-91, 93-94, and 96-98 rejected on Talbot in view of Bocci and Morgan; Claims 24-26 and 30 rejected on Talbot, Bocci, Morgan and Billstrom; Claims 31-34, 66-67 and 69 rejected on Talbot, Bocci, Morgan and Lewis; Claims 35 and 37 rejected on Talbot, Bocci, Morgan and Kniffin; Claims 44-47 and 55-58 rejected on Talbot, Bocci, Morgan, Serbetciouglu and Kniffin; Claims 36-40, 41-43, 74-76, 80, 86, 88-89, 92 and 122-123 rejected on Talbot, Bocci, Morgan and Kennedy; and Claims 49-54 rejected on Talbot, Bocci, Morgan, Kennedy and Lewis.

With respect to the rejections under 35 U.S.C. 103, various ones of the claims are amended and the following argument is presented to distinguish the claimed subject matter from the teachings of the cited art, considered individually and in combination, thereby to overcome the rejections and to show the presence of allowable subject matter in the claims. The claims are amended primarily for clarification so as to facilitate distinguishing the claimed subject matter from the teachings of the cited art, and, in the method claims, to focus on activities performed at a mobile terminal.

The Examiner maintains his rejection of all the pending claims. He states that in Bocci the light of receipt of a decrypted signal indicates that the communication has taken place in enciphered mode. The Examiner has cited a new reference Morgan and uses it together with the previously cited references Bocci and Talbot to reject all the pending claims under 35 USC § 103.

Morgan discloses a portable cryptographic device, adapted to be hand-held through solid state electronics, which possesses the capability for enciphering and deciphering plain text. The housing of the device has a keyboard for the input of plain text or cipher text, including numeric characters and control signals and, further, has a display for displaying the inputs. Circuitry within the device is responsive to the inputs and controls the display. Additional circuitry enciphers or deciphers the inputs and substitutes the resulting text into the display. The device incorporates a random code generator for generating a randomized message key which, together with the keyboard inputs, initiates and generates a long sequence of randomized letters for enciphering purposes. In a deciphering mode, a predetermined message key may be entered to set the random code generator at a point to generate the originally entered plain text. Also, a basic key composed of multiple segments fully initializes the random code generator such that more than one device could be used to encipher and decipher text. Similarly, by using different segments of the basic key, varying levels of security can be obtained. Test circuitry is also provided to insure maintenance of the proper key variables and proper operation of the device (Abstract).

Col. 2, lines 40-48 of Morgan et al. states "*In accordance with another aspect of the present invention, a cryptographic device is provided with circuitry capable of receiving a multi-input basic key to fully initialize a random code generator. In this manner, a second device may receive the same multi-input basic key to fully initialize its random code generator. The two or more devices are then synchronized and are capable of enciphering and deciphering information separately to generate logical plain text.*"

Further, on col. 5, line 20—col. 6, line 2 it reads

"*To encipher a message once the unit is loaded with the basic key, after the power switch 13 has been switched on, the decipher/encipher switch 14 is set to the encipher E position. The master reset push button 20 is then pressed, which resets the unit and places the key generator in the randomizing state. The master key push button 19 is then pressed to automatically generate and display five random message key characters. The operator then writes down these characters as the first group of*

ciphered text. At this point, the first five characters of the plain text message to be enciphered are entered via the keyboard 12 and displayed on the display 11. The equal push button 21 is then pressed to encipher the entered group and the resulting cipher text appears on the display 11. This is recorded for later transmission. Then, in the same manner, the remainder of the plain text is keyed in and enciphered in five character groupings. Each character grouping is recorded spaced from adjacent character groupings for ease of decipherment".

Further, beginning at line 50, the passage reads:

"After the entire message has been enciphered, the operator may transmit the message in any number of ways, such as over the telephone, by telex, by letter or the like. An unauthorized intercept of the message will be unable to determine the message due to the high level of encipherment provided by the system.

If the operator possesses an enciphered message and desires to decipher that message, the decipher/encipher switch 14 is set to decipher D and the message key indicated above must be entered as the first block of the five characters. This is done by pressing the master reset push button 20 and the message key push button 19, followed by entry of the five character message key code group. At this point, the equal push button 21 is pressed and the unit is ready for entry of the enciphered message. The enciphered message is entered in five character groupings, followed by pressing the equal push button 21, upon which the plain text will appear on the display 11. The recovery feature accomplished by pressing the clear entry push button 23 operates as above."

In other words, the message key push button 19 is used to generate an enciphering key to encipher a message or to enter a previously generated enciphering key to decipher a message. This is not an indication of an enciphered mode of communication. Further, the device is not capable of communicating with other devices but it is the user of the device which communicates the enciphering key and the enciphered message to

a user of another device. The user of the other device enters the key and the enciphered message to the other device which deciphers the message.

There is no indication in Morgan that the device could operate in an unenciphered mode. The characters entered to the device either constitute the deciphering key or belong to the message to be enciphered. Further, the enciphering key displayed by the device is in no way indicating that a mobile communication network is configured to use an enciphered mode of communication. For example, if the user of the device decided to send the enchipered message (displayed by the device in groups of five characters) by using a facsimile, the facsimile would not encipher the message unless the telephone network is configured to use enciphered mode of communication. However, in the system of Morgan et al. there is not provided any teaching regarding indication of a ciphered mode of communication of the telephone network or sending a cipher mode control signal from the mobile communication network to the mobile station. The device disclosed by Morgan et al is totally independent of an enciphering mode whatsoever of a communication network. On the basis of the above arguments, the Morgan et al reference fails to teach the presently claimed subject matter even if combined with Bocci and Talbot.

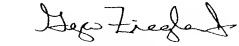
As to the Bocci reference and the Examiner's argumentation, the applicant respectfully disagrees. Bocci does not teach *sending from the mobile communication network to the mobile station a cipher mode control signal, the cipher mode control signal for setting the mobile station into an enciphered mode of communication*. According to Bocci, a receiver includes a plurality of encode-decode modules (12, 14, 16), placed in parallel, each of which is adapted to decrypt a received signal according to a respective one of three keys (1, 2 or 3) available to the receiver (column 3, lines 23 to 32). The output of each encode-decode module is taken to a corresponding delta-modulation detector (18, 20, 22). The display unit 28 is adapted to display a visual indication, such as a light, in response to a signal from the particular delta-modulation detector 18, 20 or 22. Illumination of a particular light serves to signal that a received encrypted signal has been successfully decrypted using a particular key (column 3, lines 59 to 63). There is

no indication in Bocci that a cipher mode control signal could have been transmitted and that the mobile station is set into an enciphered mode of communication if the cipher mode control signal have been detected.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment of $210 for one additional independent claim in excess of three, $450 for nine additional total claims, $1050 for a 3-month extension of time, and for any other fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Geza C. Ziegler, Jr.
Reg. No. 44,004

9 April 2008
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512